Afghanistan

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 05 May 2020

[reference to the provisions of the Budapest Convention]

Chapter I – Use of terms

Article 1 – "Computer system", "computer data", "service provider", "traffic data"

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Article 2 – Illegal access
Article 3 – Illegal interception
Article 4 – Data interference
Article 5 – System interference
Article 6 – Misuse of devices
Article 7 – Computer-related forgery
Article 8 – Computer-related fraud
Article 9 – Offences related to child pornography
Article 10 – Offences related to infringements of copyright and related rights
Article 11 – Attempt and aiding or abetting
Article 12 – Corporate liability
Article 13 – Sanctions and measures

Section 2 – Procedural law

Article 14 – Scope of procedural provisions
Article 15 – Conditions and safeguards
Article 16 – Expedited preservation of stored computer data
Article 17 – Expedited preservation and partial disclosure of traffic data
Article 18 – Production order
Article 19 – Search and seizure of stored computer data
Article 20 – Real-time collection of traffic data
Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

Chapter III – International co-operation

Article 24 – Extradition
Article 25 – General principles relating to mutual assistance
Article 26 – Spontaneous information
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
Article 28 – Confidentiality and limitation on use
Article 29 – Expedited preservation of stored computer data
Article 30 – Expedited disclosure of preserved traffic data
Article 31 – Mutual assistance regarding accessing of stored computer data
Article 32 – Trans-border access to stored computer data with consent or where publicly available
Article 33 – Mutual assistance in the real-time collection of traffic data
Article 34 – Mutual assistance regarding the interception of content data
Article 35 – 24/7 Network

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**Penal Code 2017** "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and includes any removable storage medium which is for the time being in the computer system, and a computer system is to be regarded as containing any program or data held in any such medium; "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; "program or computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function; "service provider" includes: (i) a person acting as a service provider in relation to sending, receiving, storing or processing of electronic communication or the provision of other services in relation to electronic communication through any electronic system; (ii) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; (iii) any other person who processes or stores data on behalf of such electronic communication service or users of such service; or (v) any person who, as a core business or a substantial part of his business, provides a network for distribution of electronic communication;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Penal Code 2017** **Article 122: Illegal access to computer system** (1) Whoever intentionally, whether temporary or not,— (a) causes a computer system to perform any function with intent to secure access to the whole or any part of any computer system or to enable any such access to be secured; (b) the access he intends to secure or to enable to be secured is unauthorized under this article; and (c) at the time when he causes the computer system to perform the function he knows that the access he intends to secure or to enable to be secured is unauthorized under this article, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. Explanation.-The absence of authority in this article will also include instances where there may exist general authority to access a computer system but a specific type, nature or method of access may not be authorised.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Penal Code 2017** **Article 125: Unauthorized interception** 1) Whoever intentionally commits unauthorized interception by technical means of- (a) any transmission that is not intended to be and is not open to the public to, from or within a computer system; or (b) electromagnetic emissions from a computer system that are carrying data, shall be punished with imprisonment of either description for a term which may extend to [to be specified]or with fine which may extend to [to be specified] or with both: Provided that it shall not be an offence if interception is undertaken in compliance of and in accordance with the terms of a warrant issued under this Act any law or if lawfully conducted by any intelligence agency or intelligence service article:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Provided further that this article shall not have any application upon the activities and functions of intelligence agencies or services and is without prejudice to national security requirements. (2) Whoever commits an offence under sub-article (1) fraudulently, dishonestly or with similar intent shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (3) Whoever commits an offence under sub-article (2) fraudulently, dishonestly or with similar intent - (a) for wrongful gain; or (b) for wrongful loss; or (c) for any economic benefit for oneself or for another person, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Penal Code 2017** **Article 127: Illegal interference with program or data** 1) Whoever intentionally, whether temporarily or not, — (a) does any unauthorised act in relation to a computer system; (b) at the time when he does the act he knows that it is unauthorised; and (c) acts with intent— (i) to destroy, damage, delete, erase, deteriorate, generate, modify or alter any program or data; (ii) to render any program or data inaccessible, meaningless, useless or ineffective; (iii) to obstruct, interrupt or interfere with any program or data or any aspect or attribute related to the program or data; (iv) to obstruct, interrupt or interfere with any person in the use of any program or data or any aspect or attribute related to the program or data; (v) to deny, prevent, suppress or hinder access to any program or data to any person entitled to it; (vi) to deny, prevent, suppress or hinder access to any program or data or any aspect or attribute related to the program or data or make it inaccessible; (vii) to impair the operation of any program or any aspect or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	attribute related to the program; (viii) to impair the reliability of any data or any aspect or attribute related to the data; (ix) to impair the security of any program or data or any aspect or attribute related to the program or data; or (x) to enable any of the things mentioned in sub-clauses (i) to (ix) to be done, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both.. (2) Whoever recklessly, whether temporarily or not, — (a) does any unauthorised act in relation to a computer system; (b) at the time when he does the act he knows that it is unauthorised; and (c) acts recklessly thereby– (i) causing destruction, damage, deletion, erasure, deterioration generation, modification or alteration of any program or data or any aspect or attribute related to the program or data; (ii) rendering any program or data meaningless, useless or ineffective; (iii) obstructing, interrupting or interfering with the use of any program or data or any aspect or attribute related to the program or data; (iv) obstructing, interrupting or interfering with any person in the use of any program or data or any aspect or attribute related to the program or data; (v) causing denial, prevention, suppression or hindrance of access to program or data or any aspect or attribute related to the program or data to any person entitled to it; (vi) causing denial, prevention, suppression or hindrance of access to any program or data or any aspect or attribute related to the program or data; (vii) causing impairment to the operation of any program; (viii) causing impairment to the reliability of any data or any aspect or attribute related to the program or data; (ix) causing impairment to the security of any program or data or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	any aspect or attribute related to the program or data; (x) causing enablement of any of the things mentioned in sub-clauses (i) to (ix) to be done, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified]or with both. (3) Whoever commits any offence under sub-article (1) by circumventing or infringing security measures with respect to any computer system, program or data shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (4) Whoever commits any offence under sub-article (2) by circumventing or infringing security measures with respect to any computer system, program or data shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (5) Whoever commits any offence under sub-article (1) with respect to any critical infrastructure computer system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (6) Whoever commits any offence under sub-article (2) with respect to any critical infrastructure computer system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (7) The intention referred to in sub-article (1) or the recklessness referred to in sub article (2) need not relate to— (a) any particular computer system; (b) any particular program or data; or (c) a program or data of any particular kind.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**Penal Code 2017** **Article 128: Illegal interference with computer system** 1) Whoever intentionally, whether temporarily or not, — (a) does any unauthorised act in relation to a computer system; (b) at the time when he does the act he knows that it is unauthorised; and (c) acts with intent to severely— (i) interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct the functioning of a computer system; (ii) interfere, hinder, damage, prevent, suppress, deteriorate, impair or obstruct communication between or with a computer system; (iii) interfere with or hinder access to any computer system; (iv) impair the operation of any computer system; (v) impair the reliability of any computer system; (vi) impair the security of any computer system; or (vii) to enable any of the things mentioned in sub-clauses (i) to (vi) to be done shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (2) Whoever recklessly, whether temporarily or not, — (a) does any unauthorised act in relation to a computer system; (b) at the time when he does the act he knows that it is unauthorised; and (c) acts recklessly thereby causing severe– (i) interference, hindrance, damage, prevention, suppression, deterioration or obstruction to the functioning of a computer system; (ii) interference, hindrance, damage, prevention, suppression, deterioration, impairment or obstruction of communication between or with a computer system; (iii) interference or hindrance to the access of any computer system; (iv) impairment to the operation of any computer system; (v) impairment to the reliability of any computer system; (vi) impairment to the security of any computer system: or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(vii) to enable any of the things mentioned in sub-clauses (i) to (vi) to be done shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend [to be specified] or with both. (3) Whoever commits any offence under sub-article (1) by circumventing or infringing security measures with respect to any computer system, program or data shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (4) Whoever commits any offence under sub-article (2) by circumventing or infringing security measures with respect to any computer system, program or data shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (5) Whoever commits any offence under sub-article (1) with respect to any critical infrastructure computer system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (6) Whoever commits any offence under sub-article (2) with respect to any critical infrastructure computer system, program or data that performs a critical public function shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (7) Whoever commits any offence under sub-article (1) (a) with respect to any Government controlled or public computer system, program or data that performs a public function ; and (b) that causes serious damage, injury or disruption to a widely and publicly utilised network of computer systems, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (8) Whoever commits any offence under sub-article (2) - (a) with respect to any Government controlled or public computer system,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	program or data that performs a public function ;and (b) that causes serious damage, injury or disruption to a widely and publicly utilised network of computer systems, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (9) The intention referred to in sub-article (1), or the recklessness referred to in sub-article (2), need not relate to— (a) any particular computer system; (b) any particular program or data; or (c) a program or data of any particular kind.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.	**Penal Code 2017** **Article 129: Making, supplying or obtaining devices for use in offence** (1) Whoever produces, makes, generates, adapts for use any device intending it primarily be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under Article *[Illegal access to computer system]*, Article *[Illegal access to program or data]*, Article *[Unauthorized interception],* Article *[Illegal interference with program or data],* Article *[Illegal interference with computer system]*, Article *[Electronic forgery]*, Article *[Electronic fraud]*, or Article *[Of abetments, aids or attempts to commit offence]*, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (2) Whoever transfers, imports, exports, distributes, shares, supplies, offers to supply or otherwise makes available any device believing that it is to be primarily used to commit or to assist in the commission of an offence under Article *[Illegal access to computer system]*, Article *[Illegal access to program or data]*, Article *[Unauthorized interception],* Article *[Illegal interference with program or data],* Article *[Illegal interference with computer system]*, Article *[Electronic forgery]*, Article *[Electronic fraud]*, or Article *[Of abetments, aids or attempts to commit offence]*, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	may extend to [to be specified] or with both. (3) Whoever acquires, obtains or procures any device with a view to its being supplied for primarily to be used to commit or to assist in the commission of an offence under Article *[Illegal access to computer system]*, Article *[Illegal access to program or data]*, Article *[Unauthorized interception],* Article *[Illegal interference with program or data],* Article *[Illegal interference with computer system]*, Article *[Electronic forgery]*, Article *[Electronic fraud]*, or Article *[Of abetments, aids or attempts to commit offence]*, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both: Provided that it shall not be an offence under this article- (a) where the production, making, adaptation, sale, procurement for use, import, distribution or otherwise making available of such device referred to in this article is not for the purpose of committing an offence under this Act: or any act under this article is for the authorised training, testing or protection of a computer system.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Penal Code 2017** **Article 130: Electronic forgery** (1) Whoever, through an unauthorised act, inputs, generates, alters, modifies, deletes or suppresses data, resulting in inauthentic data or an inauthentic program with the intent that it be considered or acted upon, by any person or a computer system, as if it were authentic or genuine, regardless whether or not the data is directly readable and intelligible, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (2) Whoever commits an offence under sub-article (1), dishonestly or with similar intent, (a) for wrongful gain;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) for wrongful loss; or (c) for any economic benefit for oneself or for another person, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both. (3) Whoever commits an offence under sub-article (1), fraudulently, dishonestly or with similar intent, - (a) to influence a public servant in the exercise of a public duty or function; or (b) to influence a Government controlled computer system or public computer system in exercise of a public function, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both.
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Penal Code 2017** **Article 131: Electronic fraud** Whoever with fraudulent or dishonest intent, through an unauthorised act, causes loss, in whole or in part, of any data or program, property, valuable security or consideration to another person or any computer system by- (a) any illegal access to computer system or illegal access to program or data; (b) any input, alteration, modification, deletion, suppression or generation of any program or data; (c) any interference, hindrance, impairment or obstruction with the functioning of a computer system; or (d) copying, transferring or moving any data or program to any computer system, device or storage medium other than that in which it is held or to a different location in the any other computer system, device or storage medium in which it is held; or uses any data or program; or has any data or program output from the computer system in which it is held, whether by having it displayed or in any other manner; with fraudulent or dishonest intent to procure any economic benefit for oneself or for another person,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**Penal Code 2017** **Article 136: Child pornography** 1)Whoever, intentionally, does any of the following acts: (a) publishes child pornography through a computer system; or (b) produces child pornography for the purpose of its publication through a comp uter system; or (c) possesses child pornography in a computer system or on a computer data storage medium; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. (2) It is a defence to a charge of an offence under paragraph (1) (a) or (1)(c) if the person establishes that the child pornography was a bona fide scientific, research, medical or law enforcement purpose. (3) In this section: "child pornography" includes material that visually depicts: (a) a minor engaged in sexually explicit conduct; or (b) a person who appears to be a minor engaged in sexually explicit conduct; or (c) realistic images representing a minor engaged in sexually explicit conduct. "minor" means a person under the age of [x] years. "publish" includes: (a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	any way; or (b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or (c) print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in paragraph (a).
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Penal Code 2017** **Article 132: Offences related to infringements of copyright and related rights** (1) Whoever through input, alteration, modification, deletion, suppression or generation of any program or data or through use of any computer, computer system or electronic device commits any offence under Article 31 of the "Law on the support the right of authors, composers, artists and researchers (Copy Right Law)", No. 54 of 21st July 2008, shall be punished with imprisonment of either description for a term which may extend to [to be specified] or with fine which may extend to [to be specified] or with both.
Title 5 – Ancillary liability and sanctions	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**Penal Code 2017** **Article 138: Abetments and Attempts Punishable as Offences** (1) Any person who knowingly and wilfully abets the commission of, who aids to commit or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Chapter shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence. (2) For an offence to be committed under this article, it is immaterial where the act in question took place.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Penal Code 2017** **Article 139: Offence by Body Corporate** 1. Where an offence under this Chapter, is committed for the benefit of a legal person by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: (a) power of representation of the legal person; (b) an authority to take decisions on behalf of the legal person; (c) an authority to exercise control within the legal person the legal person shall be liable for the offence and punished with fine which may extend to [to be specified] 2 Where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence under this Chapter, for the benefit of a legal person by a natural person acting under its authority the legal person shall be held liable for the offence and punished with fine which may extend to [to be specified]. 3 Notwithstanding the above, such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents